UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA

v.

LAURI LOVE,

also known as "nsh",
also known as "route",
also known as "peace",
also known as "shift",

Defendant

Criminal No. 1:14-cr-258

Count 1: 18 U.S.C. § 371
Conspiracy

Counts 2 through 7: 18 U.S.C. § 1030(a)(5)(A) and § 2, Damage to a Protected Computer and Aiding and Abetting

Count 8: 18 U.S.C. § 1029(a)(3) and § 2
Access Device Fraud and Aiding and Abetting

Count 9: 18 U.S.C. § 1028A(a)(1) and § 2
Aggravated Identity Theft and Aiding and Abetting

Notice of Forfeiture

SUPERSEDING INDICTMENT

May 2015 TERM — at Alexandria, Virginia

Introduction

THE GRAND JURY CHARGES THAT:

At all times relevant to this Indictment:

1. The defendant, LAURI LOVE, was a citizen of the United Kingdom who resided in or near Stradishall, England. As set forth more fully below, LOVE specialized in gaining unauthorized access to protected computers and obtaining sensitive and confidential information stored on those computers, including names, social security numbers, and credit card numbers.

2. LOVE was also known as "nsh", "route", "peace", and "shift".

3. The Department of Health and Human Services ("HHS") was a cabinet-level department in the executive branch of the United States Government. Its principal purpose was to protect the health of all Americans and provide essential medical services. The Health

Resources and Services Administration ("HRSA") was an agency of HHS and was responsible for providing access to health care for people who are uninsured, isolated, or medically vulnerable. The National Institutes of Health ("NIH") was an agency of HHS and was the largest source of funding for medical research in the world. The Food and Drug Administration ("FDA") was an agency of HHS and was responsible for protecting public health through the regulation and supervision of medical products, drugs, tobacco, and the nation's food supply.

4. The United States Sentencing Commission ("USSC") was an independent agency in the judicial branch of the United States Government. Its principal purposes were to establish sentencing policies and practices for the federal courts, including guidelines to be consulted regarding the appropriate form and severity of punishment for offenders convicted of federal crimes; to advise and assist Congress and the executive branch in the development of effective and efficient crime policy; and to collect, analyze, research, and distribute a broad array of information on federal crime and sentencing issues, serving as an information resource for Congress, the executive branch, the courts, criminal justice practitioners, the academic community, and the public.

5. The Regional Computer Forensics Laboratory ("FBI–RCFL") was a national forensics laboratory and training center devoted to the examination of digital evidence in support of criminal investigations. The Federal Bureau of Investigation oversaw the operations of the various RCFL offices.

6. The Department of Energy ("DOE") was a cabinet-level department in the executive branch of the United States Government. Its mission was to ensure America's security and prosperity by addressing its energy, environmental, and nuclear challenges through science and technology solutions.

7. Deltek, Inc. was a corporation headquartered in Herndon, Virginia, that provided information technology services to government contractors.

8. Forte Interactive, Inc. was a corporation headquartered in West Palm Beach, Florida, that provided web services for nonprofits.

9. Victims D.P., J.E., B.H., and J.K. are individuals who were residents of the Eastern District of Virginia and are known to the Grand Jury.

10. The above introductory allegations are realleged and incorporated in each count of this Indictment as though fully set out in each count.

COUNT 1

Conspiracy — 18 U.S.C. § 371

THE GRAND JURY FURTHER CHARGES THAT:

11. Beginning in at least October of 2012 and continuing until at least the date of this Indictment, in the Eastern District of Virginia and elsewhere, the defendant, LAURI LOVE, knowingly and intentionally conspired and agreed with unindicted conspirators known and unknown to the Grand Jury, to commit an offense against the United States, that is:

a. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage, and attempt to cause damage, without authorization, to a protected computer, with such damage and attempted damage causing loss to victims during any 1-year period, including loss resulting from the course of conduct affecting protected computers, aggregating at least $5,000 in value, and causing damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, and national security; in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(A)(i)(I), (c)(4)(A)(i)(V), and (c)(4)(B); and

b. to knowingly and with intent to defraud possess fifteen or more devices which are unauthorized access devices, in violation of Title 18, United States Code, Section 1029(a)(3).

Manner and Means of the Conspiracy

It was part of the conspiracy that:

12. The defendant, LAURI LOVE, together with conspirators known and unknown to the Grand Jury, planned and executed a series of computer intrusions against victim websites. LOVE and his conspirators gained unauthorized access to the protected computers that hosted the websites by exploiting a vulnerability in Adobe ColdFusion. ColdFusion is computer software designed to build and administer websites and databases. The vulnerability, which has since been corrected, allowed LOVE and his conspirators to access protected areas of the victims' computer servers without proper login credentials — in other words, to bypass security on the protected computers without authorization.

13. LOVE and his conspirators planned and discussed these computer intrusions, sometimes in real time while committing the offenses, in dedicated online chatrooms known as Internet Relay Chat ("IRC") channels. In these online chatrooms, LOVE used the online nicknames "nsh", "route", "peace", and "shift".

14. LOVE and his conspirators identified potential victim websites by executing computer programs designed to search the Internet for websites susceptible to being attacked through the ColdFusion vulnerability. After identifying vulnerable websites, LOVE's computer program automatically uploaded files — known as "shells" or "back doors" — to the computer servers hosting the websites. These shells were password-protected and served as custom file managers for ColdFusion applications running on the protected computer servers. After identifying a website as vulnerable, the program outputted the phrase "BEWM" followed by the website domain. LOVE and his conspirators accessed the file managers through ordinary web browsers. The file managers provided LOVE and his conspirators with administrator-level access

to the protected computer servers, which included the capabilities of uploading and downloading files, as well as creating, editing, removing, and searching for data

15. After gaining unauthorized access to the victim's protected computers, LOVE and his conspirators obtained massive amounts of sensitive and confidential information stored on those computers. LOVE and his conspirators unlawfully obtained from the victims identified in this Indictment more than 100,000 employee records, including names, social security numbers, addresses, phone numbers, and salary information, and more than 100,000 financial records, including credit card numbers and names, and caused loss aggregating in excess of $5 million.

Overt Acts

In furtherance of the conspiracy and to effect the objects of the conspiracy, the following overt acts, among others, were committed in the Eastern District of Virginia and elsewhere by members of the Conspiracy:

16. On or about December 24, 2012, LOVE uploaded without authorization backdoor shells to the domains ask.hrsa.gov and accessdata.fda.gov. That same day, LOVE wrote the following in an IRC chatroom: "BEWM: www.ask.hrsa.gov" and "BEWM: www.accessdata.fda.gov". Also that same day, LOVE wrote the following in an IRC chatroom using the online nickname "shift": "Trying to pwn [http://www.ask.hrsa.gov]". After successfully gaining unauthorized access to the protected computer, LOVE wrote: "oh so much to do . . . i will behave though and not autopwn many . . . because need to keep technique under wraps . . . ." The word "pwn" is a slang term for gaining access to, or control of, a system. At that time, computer servers hosting the domain ask.hrsa.gov were located in the Eastern District of Virginia.

17. On or about December 24, 2012, LOVE wrote the following in an IRC chatroom: "BEWM: www.ussc.gov". The following day, on or about December 25, 2012, LOVE uploaded

without authorization a backdoor shell to the domain www.ussc.gov. At that time, computer servers hosting the domain www.ussc.gov were located in the Eastern District of Virginia.

18. On or about January 11, 2013, LOVE uploaded without authorization a backdoor shell to the domain rcfl.gov. That same day, LOVE unlawfully obtained from rcfl.gov confidential and sensitive data and property belonging to the Federal Bureau of Investigation Regional Computer Forensics Laboratory. On or about the next day, LOVE wrote the following in an IRC chatroom using the online nickname "peace": "who's the motherfucking biatch naooo?!?" followed by the backdoor location on the FBI–RCFL website. At that time, computer servers hosting the domain rcfl.gov were located in the Eastern District of Virginia.

19. On or about January 14, 2013, LOVE uploaded without authorization another backdoor shell to the domain www.ussc.gov.

20. On or about January 16, 2013, LOVE wrote the following in an IRC chatroom using the online nickname "peace": "www.ussc.gov . . . has been under our control for, well, an undisclosed period of time".

21. On or about January 17, 2013, LOVE uploaded without authorization a backdoor shell to the domain report.nih.gov.

22. On or about January 22, 2013, LOVE unlawfully obtained from rcfl.gov additional confidential and sensitive data and property belonging to FBI–RCFL. LOVE obtained from FBI–RCFL employee email addresses and documents.

23. On or about January 24, 2013, LOVE unlawfully obtained from www.ussc.gov confidential and sensitive data and property belonging to the United States Sentencing Commission's hosting provider, Circle Solutions, including internal business documents, correspondence, and meeting minutes. Also that day, LOVE wrote the following in an IRC

chatroom using the online nickname "route": "i'm just trying to get as much as possible before drop . . . because [the hosting provider] will lock their shit down . . . ."

24. On or about February 11, 2013, LOVE wrote the following in an IRC chatroom using the online nickname "peace": "remote computer forensics lab . . . is fbi site . . . can probably get good infos from people who use . . . ."

25. On or about July 3, 2013, LOVE uploaded without authorization a backdoor shell to the domain iq.govwin.com. That same day, LOVE unlawfully obtained from iq.govwin.com confidential and sensitive data and property belonging to Deltek, Inc., including financial and employee access information. The financial information included approximately 23,000 credit card numbers and the associated names, and the employee access information included approximately 80,000 usernames and passwords. At that time, computer servers hosting the domain iq.govwin.com were located in the Eastern District of Virginia.

26. On or about July 4, 2013, LOVE wrote the following in an IRC chatroom using the online nickname "peace": "it worked . . . we have . . . easily 5-10k contractor and gov credit cards . . . ."

27. On or about July 10, 2013, LOVE wrote the following in an IRC chatroom using the online nickname "peace": "man this govwin site is really useful . . . they do breakdowns of spending for all gov agencies . . . org charts . . . related documents . . . related articles . . . we need like a team of lots of people poring over this data . . . ."

28. On or about July 24, 2013, LOVE uploaded without authorization a backdoor shell to the domain mis.doe.gov.

29. On or about July 26, 2013, LOVE unlawfully obtained from mis.doe.gov confidential and sensitive data and property belonging to the U.S. Department of Energy

("DOE"), including all of the information maintained in the internal databases related to DOE employees, contractors, and visitors. The information included names, social security numbers, dates of birth, phone numbers, work and personal email addresses, and salary information. Hundreds of these individuals were at that time residents of the Eastern District of Virginia. That same day, LOVE wrote the following in an IRC chatroom using the online nickname "peace": "this is why you never give up h4xing https://mis.doe.gov/[REDACTED]". LOVE also wrote: "searching department of energy employee records", and he shared in the IRC chatroom the personal information of various DOE employees, including names, addresses, phone numbers, and work and personal email addresses. LOVE also wrote: "YASSSS" "I AM INVINCIBLE!!!" "(finally shelled mis.doe.gov after over 24h)".

30. On or about July 29, 2013, LOVE wrote the following in an IRC chatroom using the online nickname "peace": "just finished snarf/decrypt/format all the valid CC's from govwin". That same day, LOVE uploaded to a computer server a spreadsheet containing information obtained from iq.govwin.com, including names, job titles, addresses, phone numbers, and approximately 23,000 credit cards numbers with expiration dates and items purchased. Other members of the conspiracy obtained copies of the spreadsheet from the server on or about January 24, 2014, and on or about March 10, 2014.

31. On or about July 31, 2013, LOVE wrote the following in an IRC chatroom using the online nickname "peace": "It's basically every piece of information you need to do full identify theft on any employee or contractor for the Department of Energy."

32. On or about August 14, 2013, LOVE uploaded without authorization a backdoor shell to a computer server known to the Grand Jury. That same day, LOVE unlawfully obtained from that computer server confidential and sensitive data and property belonging to

Forte Interactive, Inc., including names, addresses, phone numbers, email addresses, and credit card numbers with expiration dates and items purchased. Hundreds of these individuals were at that time residents of the Eastern District of Virginia. That same day, LOVE wrote the following in an IRC chatroom using the online nickname "peace": "just found half a million credit card numbers (valid)". He also wrote that the conspirators needed to come up with a way of "committing massive credit card fraud" and that the conspirators had become "rich(er) in theory".

33. On or about October 1, 2013, LOVE wrote the following in an IRC chatroom using the online nickname "route": "also we can set up a whole bunch of people ready to make CC purchases . . . for the govwin cards". A conspirator responded, "banks will be hit with the bill".

All in violation of Title 18, United States Code, Section 371.

COUNTS 2–7

Damage to a Protected Computer and Aiding and Abetting — 18 U.S.C. § 1030(a)(5)(A) and § 2

THE GRAND JURY FURTHER CHARGES THAT:

34. The factual allegations contained in Count 1 are realleged and incorporated by reference here.

35. On or about the following instances, each instance constituting a separate count, in the Eastern District of Virginia and elsewhere, the defendant, LAURI LOVE, knowingly caused the transmission of a program, information, code, and command, and aided and abetted others in doing so, and as a result of such conduct, intentionally caused damage, and attempted to cause damage, without authorization, to a protected computer, with such damage and attempted damage causing loss to victims during any 1-year period, including loss resulting from the course of conduct affecting protected computers, aggregating at least $5,000 in value, and causing damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, and national security:

COUNT	APPROXIMATE DATE	VICTIM
2	December 24, 2012	U.S. Department of Health and Human Services
3	December 25, 2012	United States Sentencing Commission
4	January 11, 2013	FBI Regional Computer Forensics Laboratory
5	July 3, 2013	Deltek, Inc.
6	July 24, 2013	U.S. Department of Energy
7	August 14, 2013	Forte Interactive, Inc.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(A)(i)(I), (c)(4)(A)(i)(V), (c)(4)(B), and 2.

COUNT 8

Access Device Fraud and Aiding and Abetting — 18 U.S.C. § 1029(a)(3) and § 2

THE GRAND JURY FURTHER CHARGES THAT:

36. The factual allegations contained in Counts 1 through 7 are realleged and incorporated by reference here.

37. On or about July 29, 2013, in the Eastern District of Virginia and elsewhere, the defendant, LAURI LOVE, knowingly and with intent to defraud, possessed 15 or more unauthorized access devices, and aided and abetted others in doing so, said possession affecting interstate and foreign commerce, in that the defendant, from a location outside the United States, obtained thousands of unauthorized access devices by accessing without authorization a protected computer located inside the United States, and stored the unauthorized access devices in multiple locations, including a location outside the United States.

All in violation of Title 18, United States Code, Sections 1029(a)(3), (c)(1)(a)(i), and 2.

COUNT 9

Aggravated Identity Theft and Aiding and Abetting — 18 U.S.C. § 1028A(a)(1) and § 2

THE GRAND JURY FURTHER CHARGES THAT:

38. The factual allegations contained in Counts 1 through 8 are realleged and incorporated by reference here.

39. On or about July 3 and 4, 2013, in the Eastern District of Virginia and elsewhere, the defendant, LAURI LOVE, did knowingly transfer, possess, and use, and aided and abetted others in doing so, without lawful authority, a means of identification of another person, namely, thousands of individuals' names and credit card information, including Victims D.P., J.E., B.H., and J.K., as well as thousands of individuals' usernames and passwords, during and in relation to the Damage to a Protected Computer offense charged in Count 5 of this Indictment.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

NOTICE OF FORFEITURE

18 U.S.C. §§ 981, 982, 1029, and 1030; 21 U.S.C. § 853; and 28 U.S.C. § 2461

40. The allegations contained in Counts 1 through 9 of this Indictment are realleged and incorporated by reference for the purpose of alleging forfeiture.

THE GRAND JURY HEREBY FINDS THAT:

41. There is probable cause that the property described in this NOTICE OF FORFEITURE is subject to forfeiture pursuant to the statutes described herein.

42. Pursuant to Federal Rule of Criminal Procedure 32.2(a), the United States of America gives notice to the defendant, LAURI LOVE, that, in the event of his conviction of any of the offenses charged in Counts 1 through 9 of this Indictment, the United States intends to forfeit the defendant's property as further described in this NOTICE OF FORFEITURE.

43. Upon conviction of a conspiracy to violate 18 U.S.C. §§ 1029 and 1030, in violation of 18 U.S.C. § 371, as set forth in Count 1 of this Indictment, the defendant, LAURI LOVE, shall forfeit to the United States of America any property, real or personal, which constitutes or is derived from proceeds traceable to the violations, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c).

44. Upon conviction of any of the computer fraud offenses in violation of 18 U.S.C. § 1030, as set forth in Counts 2 through 7 of this Indictment, or upon conviction of the conspiracy to violate 18 U.S.C. § 1030, in violation of 18 U.S.C. § 371, as set forth in Count 1 of this Indictment, the defendant, LAURI LOVE, shall forfeit to the United States of America:

a. pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i), any property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violation; and

b. pursuant to 18 U.S.C. § 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of such violation, and any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

45. Upon conviction of the offense in violation of 18 U.S.C. § 1029, as set forth in Count 8 of this Indictment, the defendant, LAURI LOVE, shall forfeit to the United States of America:

a. pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1029(c), any property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violation; and

b. pursuant to 18 U.S.C. § 1029(c)(1)(C), any personal property used or intended to be used to commit the offense.

SUBSTITUTE ASSETS

46. If any of the property described above, as a result of any act or omission of the defendant, LAURI LOVE,

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to and intends to seek forfeiture of substitute property pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. §§ 982(b)(1), 1029(c)(2), and 1030(i)(2), and 28 U.S.C. § 2461(c).

All pursuant to 18 U.S.C. §§ 981, 982, 1029, and 1030; 21 U.S.C. § 853; and 28 U.S.C. § 2461.

A TRUE BILL:

Foreperson
United States Grand Jury

Respectfully submitted,

Dana J. Boente
United States Attorney

By: _____
Jay V. Prabhu
Assistant U.S. Attorney

Ryan K. Dickey
Special Assistant U.S. Attorney
Senior Counsel, Computer Crime and Intellectual Property Section
U.S. Department of Justice, Criminal Division